JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 3(2), 2017, 91–108
doi: 10.1093/cybsec/tyx009
Advance Access Publication Date: 26 December 2017
Research paper

Research paper

Strategic news bundling and privacy breach disclosures

Sebastien Gay*

Georgetown University, Department of Economics, Washington DC, 20057, USA

*Corresponding author. E-mail: sebastien.gay@georgetown.edu

Received 21 August 2017; accepted 23 October 2017

Abstract

I examine how firms strategically bundle news reports to offset the negative effects of a privacy breach disclosure. Using a complete dataset of privacy breaches from 2005 to 2014, I find that firms experience a small and significant 0.27% decrease in their stock price on average following the breaking news disclosure of the privacy breach. But controlling for media coverage, this small decline is offset by an increase in the effect of a larger than usual number of positive news reports released by the firm on that day, which could increase the returns by 0.47% for every additional positive news report compared to their usual media coverage. I further find that disclosure laws have a significant and negative effect on the returns, even when news releases are used to alleviate the decrease. Moreover, a portfolio constructed with breached firms controlling for state disclosure laws outperforms the market over the 2007–14 period, especially in the case of breached firms in mandatory disclosure states.

Key words: news events; media; information; market efficiency; security breaches; event study; risk analysis; information breach; privacy; market valuation.

Introduction

The development of online transactions and data aggregation storage for companies has increased the risk of privacy breaches in the past 10 years. According to Privacy Rights Clearinghouse, in fact, there were more than 4540 breaches reported over the period 2005–14, compared to less than 1000 over 1995–2005 [1]. The increase is primarily due to the increased use, retention, and repackaging of data by companies.

On 4 February 2015, Anthem, Inc., one of the largest health insurance companies in the USA, announced that 80 million customers' and employees' data were stolen. Critical information (social security numbers, names, and dates of birth) for the 80 million affected people was at risk of fraudulent use, making the Anthem breach one of the largest privacy breaches in history. During the next trading day, however, the Anthem stock barely went down from its closed value of $137.6 of the day prior to the breach announcement, with intraday trading between $135.40 and $138.37 [2]. The close price represented a decrease of 0.31%, in line with the overall market decrease for the day. The Anthem stock was unaffected by this (random) event, with the stock closing at more than $145 within 2 weeks of the release of the breach. This is one of many examples of data breaches that affected a large amount of customers and their highly personal and sensitive data but did not lead to a market sellout of the firm's stock.

This article examines why stocks of breached firms do not seem to be significantly affected after reporting a privacy breach. I empirically show that firms counterbalance the effect of a privacy breach disclosure by bundling this negative and potentially costly release with more positive news reports to alleviate any expected decrease in stock value. I also find that firms tend to release the disclosure during a period when there are a smaller than usual amount of negative news reports. My analysis is reinforced by the fact that privacy breaches happen at random times for any given firm, but firms have some small leeway to time their disclosures. States have different laws regarding disclosures that can allow firms to announce the privacy breach event to customers or the state attorney general with different timeframes, usually between a day to up to 2 months after the firm discovers the breach. Moreover, privacy breaches are known to be indicative of negative news since they indicate that private information from customers or employees (or possibly both) has been stolen. Also, privacy breach disclosures, contrary to more frequent and prescheduled corporate disclosures, are good identifiable random events to test strategic (voluntary) disclosures by firms.

© The Author(s) 2017. Published by Oxford University Press.

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact journals.permissions@oup.com

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Despite not all states requiring disclosures, firms may want to disclose a privacy breach to avoid developing a negative reputation.

This empirical analysis answers two main questions using privacy breach disclosures: first, can firms counterbalance the negative effect of a privacy breach disclosure by strategi cally timing the release of more positive media coverage than usual? Second, do disclosure laws have a significant effect on the stock price of the firms that experience a privacy breach?

Motivation and literature review

The overall economic effect of privacy breaches on firm value is unclear. On one hand, privacy breaches, once revealed to the market, should decrease both consumers' and investors' confidence in the firm and affect the sales of its products. Breaches could also lead to potential high remediation costs for failing to protect private consumers data, through costly lawsuits, payments of a year of credit reporting, or simply decreases in future customer purchases [2–4]. It may also decrease new customer reach, as prospective customers may be concerned that their data will be disclosed or lost by the firm [2, 5]. Additionally, there is a risk of secondary market for stolen data that increases identity theft against customers and the overall cost for breached companies [6].

On the other hand, negative events like privacy breaches could have a positive effect for companies not often covered by the media. More specifically, firms might suffer from a short-run public relations nightmare due to the privacy breach, but might actually gain more investors and customers later on, due to their positive handling of the crisis.

In the Anthem case described above, the second day after the breach was reported, the *Wall Street Journal* reported that the stolen social security numbers of the 80 million customers were not encrypted (note that it is not required by law) [7]. Despite this breach news report, the stock opened at $136.95 and closed at $136.33, a small decrease explained mainly by an overall market pullback on the day, exceeding $150 within a month of the report.

Even if privacy breaches have long been debated in the public forum, it is a relatively under developed area in the economic and finance literature. Most academic papers analyze only their short-run effects with event studies using small datasets of privacy breaches. This article goes further by hypothesizing that privacy breach disclosures, due to their random nature, lead to firms bundling the disclosure with positive news reports to offset the negative effect on firms' values of the breach. Previous studies have shown that privacy breaches have a large negative effect on stocks of companies, making the information of a privacy breach being reflected quickly into the shares of a company due to the negative reputation and data protection effect on the business [8]. Contrary to inefficient markets where information does make it into share prices although the reaction to an announcement may be gradual, sometimes taking several years, the reaction for a privacy breach has been documented to be instant and publicized through remediation. Through this publicity, corporate reputation, which has value to an investor, may be affected [9, 10]. Based on this argument, a breach disclosure may lead to a loss of reputation that could aggravate if firms do not have a positive environment to counter negative news reports. It could be argued that if (irrational) investors take time to understand the implication of a given privacy breach, the bundling of good news may be decreased. Nonetheless, it is a dangerous bet for companies to not bundle positive news reports with a negative disclosure. Behavioral economics explains that potential customers may refrain from shopping at breached firms.

Using a novel panel dataset of privacy breaches and news events, I find that, controlling for firm and industry characteristics, breaking news reports about a privacy breach lead to a decrease in stock value of about 0.27% on the day of the disclosure of the privacy breach. I also estimate that on the day of the disclosures, abnormally high number of positive news reports would counterbalance the breach announcements in most industries, increasing stock returns on average by 0.47%, a number 20 times larger than the usual effect of an extra positive news report on any given day.[1] I also find that an abnormal number of negative news, other than the breach reports, leads to no significant effect on the day of disclosure of a breach. My findings seem to indicate that firms choose to release a privacy breach in a more positive media environment to try to counter the negative effect of the disclosure at the time.[2]

I contribute to the literature in several important ways. First, I complement the existing work on strategic disclosure literature in finance. The finance literature has ample attempts at finding the textual analysis impact on stock prices [11–13].

Bundles of news events have been nonetheless less studied and have mainly focused on how firms use positive disclosures (patent approvals) to mitigate future negative earnings reports [14–16]. This article analyzes the opposite effect, more specifically when a firm strategically mitigates a negative disclosure using positive news. The advantage of using privacy breaches is that it is not actually an event controlled by the company in terms of its occurrence, contrary to earning reports or directors' nominations. Therefore, the time of disclosure for a given privacy breach is not tied to a prescheduled future conference call. On the other hand, if firms do not act reasonably quickly in terms of disclosing a privacy breach they might face a Federal Trade Commission (hereafter FTC) or a state department of justice fine for delaying disclosure.[3] My analysis ties with Acquisti *et al.*'s study that approached the media variable considering major papers versus wire services for a limited amount of breaches [8]. This article also expands on Goel and Shawky's study that considers news information from public sources on breaches over 2004–08 [17]. My article relates to Cohen *et al.*'s study that show how firms manipulate the information flow to the market through strategic releases of news using conference calls [18]. I hypothesize that firms keep a stock of good news for unexpected bad news, depending on the type of negative events they need to address. It is efficient for firms to bundle positive news with news of a privacy breach when the number of customers affected by the breach is important and when there is potentially a high risk of more breaches within the same year. For example, Anthem increased its dividend on 28 January 2015, after excellent earnings reports. It also produced ten positive news reports on dividend increased, higher forecasts, share repurchasing, and profit beats.

1 This effect varies within industries: the financial and insurance, wholesale trade, and service industries lead to the highest decreases (between 0.58% and 1.05%).

2 Firms, if they choose to do so, may also use this privacy breach disclosure to release "smaller" negative news to the market when investors' attention is focused on the breach.

3 Most state disclosure laws require breached companies to notify customers and the state attorney general within a few months of discovery of the breach. See, e.g. the National Conference of State Legislations, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (26 May 2015).

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

It is widely assumed in the literature that firms strategically disclose information to the market around times with low perceived investor attention [19, 20]. I advocate the opposite. It is rational for firms to use high perceived attention to mitigate negative news reports using positive news. It may even be an opportunity to use this strategy to dump bad information at the same time. For example, during the Target conference call on the day of the privacy breach disclosure the company explained that sales might decrease over the few quarters following the breach [21].

A strong contribution of this article is to build an independent and complete dataset of news events. I will measure how the change in news coverage of a company due to privacy breaches will affect stock prices of breached firms [22, 23]. Second, I contribute to the literature of the economics of privacy by measuring the direct equity effect of privacy breach disclosures [8, 24–26]. Overall, previous papers have been divided on the direct short-run effect of privacy breach announcements. In particular, Acquisti *et al.* find that there is a negative and statistically significant effect of privacy breaches incidents on a firm's value with a dataset of 85 breaches over the period 1999–2004 [8]. Hovav and D'Arcy show that there is no significant effect of privacy breaches on a firm's value, examining small subsets of privacy breaches (viruses and denial of services) and using mainly event studies prior to 2003 [26]. Campbell *et al.* [24] find a small and insignificant effect on all security breaches for a dataset of 43 events. Horav and Gray [27] find that, with the limitation of studying only one firm, TJX's stock largely increased a year after the announcement of a massive consumer data breach [26]. My article builds on the existing literature by considering an expanded dataset of 745 breaches for publicly listed companies to measure the impact on the performance of the firms by themselves and its competitors, using the added effect of the "bundled" news released on the day of the announcement of the breach. More recently, with more coverage on privacy breaches, some further research investigated the risk and trends of privacy breaches [28–30].

The rest of the article is organized as follows: section "Data" presents my dataset. Section "Timing of privacy breach disclosure through media coverage" presents the timing of privacy breach disclosures and media coverage for firms. Section "News bundling and stock performance" describes the empirical strategy of news bundling and disclosures and a portfolio analysis. Section "Discussion" provides a discussion and applications of my results. Section "Conclusion" concludes.

Data

I construct a large dataset of stocks and news reports of publicly traded companies as follows. The data for stock prices comes from the Center for Research in Security Prices (CRSP). I use daily prices and number of shares outstanding for every company in the CRSP database over the period 2005–14.[4]

I use Standard Industrial Classification (SIC) industry numbers for each company from CRSP using Wharton Research Data Services.[5] I rely on the Fama–French 3-factor portfolios for estimation of abnormal returns. Daily and monthly Fama–French Factors are downloaded from Kenneth French's data library. I use the Fama–French factors considering the usual method of using the historical prices until 46 days before the events and then using those loadings calculated through the estimation window to estimate the abnormal returns.[6]

I build a novel dataset of privacy breaches and hacking from publicly available data from different privacy specialized websites. I consider privacy events from DatalossDB.org, Databreaches.net, PHIprivacy.net, and Privacy Rights Clearinghouse between 1 January 2005 and 31 December 2014. For each privacy breach event, I capture all of the critical information, including the date of the privacy breach disclosure, the affected companies, the number of affected customers, the description or type of breach, and the state(s) where the breach happened. The full dataset on privacy breaches contains 4 533 privacy breaches, but I exclusively focus on the 542 breach events that can be matched to the stock data in this article.[7] I made several adjustments on the privacy breach data. First, if a privacy breach affects multiple firms, I allocate the breach to all of the firms. Second, privacy breaches could affect a product produced by company, like Gmail, a Google, Inc. software, or iCloud, an Apple, Inc. software. In those cases, I assign the breach to the firm that provides the product. Third, if a breach references subsidiaries (like Lexis Nexis for Elsevier NV), the parent company is assigned the particular breach. The strategy behind this is to model the direct effect of reputation on the company.[8] Fourth, some companies, like Comcast, have multiple stock tickers trading on the market (CMCSA and CMCSK). In this case, I consider the effect on both stocks in the analysis.[9] The data on news events comes from the Dow Jones News Service. The dataset contains daily timed news events for all listed companies. I focus on the following types of news stories: (i) "breaking news" type of stories composed of a headline with no body text. Breaking news stories are the first news report released to the market when the privacy breach is revealed; and (ii) characterized Dow Jones news, corresponding to usual recurring firm activities, such as earnings, shareholder announcements, director nomination, and CEO nomination. I divide those news reports into positive and negative news reports based on the type of positive or negative themes in the articles. Positive news reports comprise

4 For daily observations where no closing price is available, I follow CRSP's imputation procedure and replace the daily stock price with the average of the bid and the ask prices for that stock on the particular day considered. I also use the CRSP adjusted returns to control for any stock splits.

5 CRSP preserves the timing of changes to SIC and NAICS categories for each company.

6 I consider the data on the SMB (Small Minus Big) portfolio, and the HML (High Minus Low) portfolio. SMB is the average return on three portfolios of small market-capitalization companies minus the average return on three portfolios of large market-capitalization companies. HML is the average return on two value portfolios minus the average return on two growth portfolios.

7 Note that I also only consider privacy breach data from companies that are publicly listed, despite the fact that the government, universities, and privately owned firms have the majority of the breaches historically. Nonetheless, despite having more breaches, these latter institutions or companies have fewer records breached than the publicly listed companies. It is mainly related to the fact that most of the breaches for universities result from a lost laptop or data misplaced. Government websites and data are breach more often by foreign countries. Privately held companies are most of the time due to the lack of protection as the cost might be too high to get the appropriate level of protection.

8 For example, LexisNexis is a known name in the legal or academic business but a breach on its products might have less of an effect on the stock of Elsevier NV due to the distance between the products (at least in the short-run controlling for the number of affected customers).

9 As a robustness check, I ran the analysis using only one of the stocks for each of the companies when multiple stock tickers existed.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Table 1. Number of privacy breaches per firm by industry

Number of breaches	1	2	3	4	5	6	7	8	9	10	14	15	16	Total
Mining	2	0	0	0	0	0	0	0	0	0	0	0	0	2
Construction	3	0	0	0	0	0	0	0	0	0	0	0	0	3
Manufacturing	31	10	1	4	1	0	2	0	0	2	0	0	0	51
Transportation, communication, electric, gas, and sanitary services	17	3	6	1	1	0	0	1	0	0	0	0	0	29
Wholesale trade	6	1	0	0	0	0	0	0	0	0	0	0	0	7
Retail trade	17	9	2	1	1	2	0	1	1	1	0	0	0	35
Finance, insurance and real estate	33	14	4	7	4	0	2	0	0	0	1	1	1	67
Services	19	14	7	3	0	0	0	1	0	0	0	0	0	44
Other	3	0	1	0	0	0	0	0	0	0	0	0	0	4
Total	131	51	21	16	7	2	4	3	1	3	1	1	1	242

Table 2. Number of privacy breaches by SIC industry division and type of breach

	Payment card fraud	Unintended disclosure	Hacking or malware	Insider	Non-electronic physical loss	Electronic port. device loss	Electronic stat. device loss	Unknown	Total
Mining	0	0	0	1	0	1	0	0	2
Construction	0	0	0	0	0	2	0	1	3
Manufacturing	5	10	27	18	3	39	4	3	109
Transportation, communication, electric, gas, and sanitary services	0	9	13	11	2	18	1	2	56
Wholesale trade	0	2	2	0	0	3	1	0	8
Retail trade	3	15	16	27	13	14	2	1	91
Finance, insurance and real estate	15	33	21	40	6	47	5	15	182
Services	0	13	28	11	5	22	4	2	85
Other	0	2	3	0	0	1	0	0	6
Total	23	84	110	108	29	147	17	24	542

distinguishable positive news events, like positive earnings or patent approval. Negative news reports are composed of clearly distinguishable negative news events, like lower guidance, negative earnings, or a plaintiff's lawsuit against the firm. Any event that is not clearly classified is assigned to the unclassified news reports. Those uncharacterized news reports, comprise less significant events for the firms, would require a more in-depth analysis given that they are rarely recurring news. I will consider them as "chatter" about the firm. [10]

I compute the average number of news events on a given day for a firm. For each day, I count the number of news events for each firm by category. I also use the press releases issued by the firm, both positive and negative. I use those press releases in particular to see if firms would make more positive announcements before a privacy breach disclosure. I find that firms actually tend to release on average more positive press releases the day prior to the announcements, compared to other days. I also generate a dummy variable if there is any breaking news on a given day and a privacy breach disclosure breaking news dummy whether there is any breaking news report on the day of the breach disclosure. I further consider the abnormal number of positive and negative news report, defined respectively as the deviation from the mean of the number of positive or negative news reports for the firm.[11] I make two types of adjustments on the news data: (i) I consider the news on the day when it is registered, as if it were a continuous flow of information; and (ii) I time-adjust the news by assigning every news report coming on a day after end of trading times (4 p.m. EST) or weekend to the next trading day. The second adjustment makes a clean information diffusion argument of a disclosure as stocks can then be sold at market as soon as the opening bell time (9:30 a.m. EST).

Table 1 shows the number of privacy breaches per firm and industry. I have a total of 242 firms disclosing a privacy breach.[12] Within this group, 28% are in the finance and insurance industry, 21% are in the manufacturing industry, and 15% are in the retail industry. Firms in the finance, insurance, and real estate industry represent more than a third of the firms breached multiple times. The other large group comprises companies in the retail, manufacturing, and services industries. Interestingly, three firms in finance and insurance industry are breached more than 14 times over the 2005–14 period as finance and insurance firms are known to hold more sensitive and valuable information like social security numbers and bank account numbers. Table 2 lists all of the breaches per

10 I also use those "chatter" news an extra control for robustness check.

11 I consider the averages using a year, a month, or the entire span of my sample for robustness purposes. Throughout the article, I report the results with averages over the past year for each firm.

12 Among the breaches that are actually reported, the impact seems to differ. For example, a breach on Apple is reported on average 60% more than a breach on Marriott Hotels. Breaches also differ in terms of customers' impact. For example, Iron Mountain had 800 000 records breached, Marriott Hotels has 206 000, but AT&T had only 1600 in a 2014 breach in 2014.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Table 3. Number of privacy breaches with news and breaking news reported

	News reported		Breaking news reported	
	Breaches with	Breaches without	Breaches with	Breaches without
Mining	2	0	2	0
Construction	2	1	1	2
Manufacturing	103	6	54	55
Transportation, communication, electric, gas, and sanitary services	52	4	26	30
Wholesale trade	5	3	1	7
Retail trade	84	7	40	51
Finance, insurance, and real estate	171	11	107	75
Services	80	5	28	57
Other	5	1	2	4
Total	504	38	261	281

Table 4. Proportion of events with breaking news on the day of breach

	Number of events	Mean	Standard deviation
Total	544	0.4798	0.5001
Market capitalization < 1B	48	0.0833	0.2793
1B < market capitalization < 100B	390	0.4333	0.4962
Market capitalization > 100B	106	0.8302	0.3773
Records breached < 100, 000	129	0.4031	0.4924
100 000 < records breached < 1 000 000	36	0.4722	0.5063
Records breached > 1 000 000	297	0.5286	0.5000
Mining	2	1.0000	0.0000
Construction	3	0.3333	0.5774
Manufacturing	109	0.4954	0.5023
Transportation, communication, electric, gas and sanitary services	56	0.4643	0.5032
Wholesale trade	8	0.1250	0.3536
Retail trade	91	0.4396	0.4991
Finance, insurance, and real estate	182	0.5879	0.4936
Services	85	0.3294	0.4728
Other	6	0.3333	0.5164

industry and type for each breach event. I find that most of the 542 events can be grouped into the following categories: hacking events, loss of a computer or electronic device, insider breach, and unin tended disclosures. Surprisingly, payment or credit card fraud events are a small category of privacy breaches. It may be due to a higher level of security and regulation for companies. Nonetheless, when those events happen they usually have larger records breached.

Table 3 reports the news coverage of the privacy breach disclosures for all of my 542 events. I find that 38 disclosed privacy breaches did not match with any news (or breaking news) on that day. Those breaches are either of smaller scale or in industries where the data stolen is not strategic. Moreover, more than half of the privacy breach disclosures did not get a breaking news report about the breach on the day of disclosure. This number varies with industries. For example, in the financial industry, privacy breach disclosures are reported as breaking news reports 58% of the time. I find that 281 privacy events match with disclosure days without any news report or breaking news. The sample contains 13 600, 104 news events, even with the adjustments specified above. It should be noted that all days of the week have a similar number of news reports within my sample of firms. It justifies my use of the number of abnormal news reports compared to the average number of news reports. Privacy breach disclosures happen on any days of the week per industry, with a slight bias towards the Monday release. It is mainly due to the fact that 56 of the 130 breaches are disclosed over the weekend. Therefore, their effect would only be measured on the next Monday, i.e. the first trading day after disclosure. On average there is a similar trend of breaking news reports on the day of disclosure irrespective of the week. I notice that there are more news reports at the beginning of the week than towards the end of the week. I notice that there are on average 87.7 days with breaking news reports and 132.3 days when there are no breaking news reports. Unsurprisingly, the industries with the most breaking news reports are the finance, insurance and real estate, services, manufacturing, and retail industries. Those industries get similarly more news reports on average than other ones. Breaking news reports are evenly divided over the days of the week. Not surprisingly, breaking news are reports not often released over the weekend. I assign them to the Monday news data. As a reminder all news are assigned to their trading days. For example, the Tuesday column in my tables corresponds to any news released between Monday after trading closes until Tuesday end of trading, i.e. Monday 4 p.m. until

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Tuesday 3:59 p.m. Table 4 divides the sample by market capitalization, number of records breached in the breach, and the different type of industries. I find that the larger the firm, the more likely there will be a breaking news about the breach (83% for firms larger than 100 billion dollars in market capitalization versus only 8% for firms under 1 billion dollars). Also, the higher the number of records breached, the more likely the privacy breach would be released to the market by a breaking news reports (52% for more than a million records breached versus only 40% on average for less than 100, 000). All industries seem to be given equal breaking news coverage in the case of a privacy breach, mostly between 30% and 50%.[13]

The data on security breach disclosure laws by state comes from the National Conference of State Legislatures. On 1 January 2015, 47 states had security breach laws that outline the compliance requirements of firms that are victims of privacy breaches. I will mainly consider how the laws differ from the timing of a privacy breach disclosure standpoint and when they were passed or implemented.

Timing of privacy breach disclosure through media coverage

In this article, I analyze how firms decide to bundle news strategically to the market when disclosing privacy breaches. In particular, managers have a strategic informational advantage when deciding to disclose information to the market. Part of the literature attempts to measure the effect of disclosing information when investors have limited attention. Those papers used mainly controlled and prescheduled types of events due to mandatory disclosures (earnings announcements, management forecasts, corporate changes) [19, 20]. Contrary to the nature of the events analyzed in those papers, privacy breaches are somewhat uncontrolled and unplanned events in nature. In case a breach happens, firms have to disclose the breach no later than up to 3 months of the discovery of the breach. Some states have stronger requirements (5 days in California) than others (90 days for Connecticut). Affected firms can then strategically consider when to disclose the breach within this timeframe, given that this information could be easily leaked or released in the press.

The sample statistics in section "Data" seem to suggest that firm size, media coverage, and breach size tend to have an effect on the probability of getting a breaking news report when a privacy breach is disclosed. I want to analyze more specifically the media environment firms either create (through press releases) or use (through media stories) around a negative disclosure like a privacy breach.

Fig. 1 shows the media coverage for the firms in my sample. I divide the type of news reports into positive and negative news and I also consider the breaking news reports. In order to account for different media coverage between firms,[14] I construct the following news ratios: the "abnormal news coverage" can be written as:

$$ABN_{it} = \frac{N_{it} - \overline{N_i}}{\overline{N_i}} \quad (1)$$

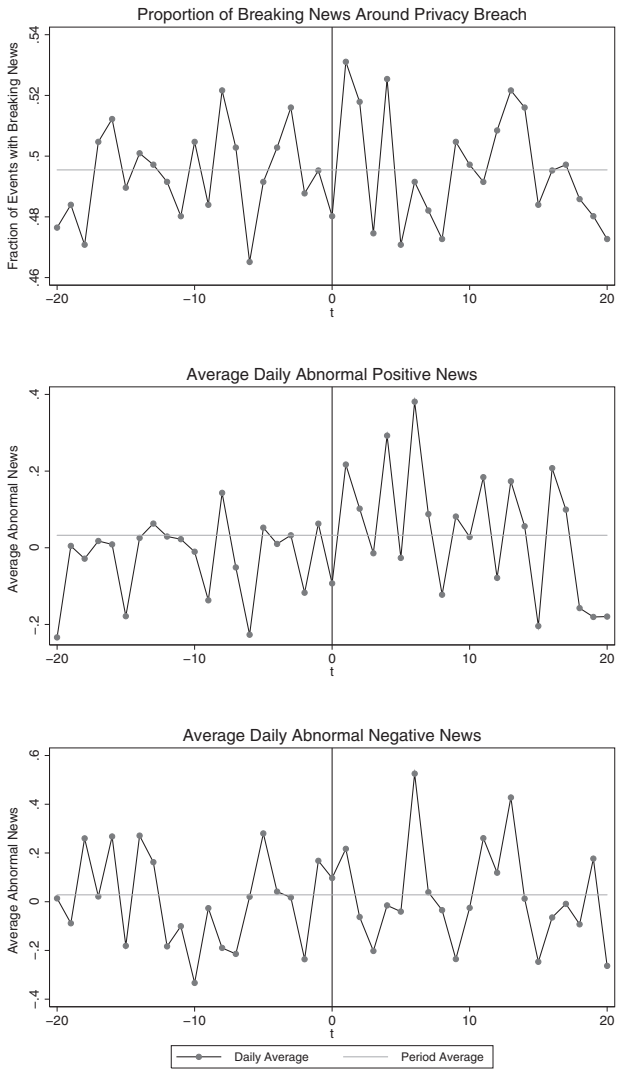

Figure 1: Media coverage of firms.

where N_{it} is the sum of news stories during day t for firm i and $\overline{N_i}$ is sum of all news stories represents the average over the time period. I consider different time periods for the measure of the "permanent news coverage" in Equation (1). The permanent news coverage of a given firm corresponds to the usual media coverage of a given firm: I use the average over the entire sample 2005–14 and average per year to better control to changes in company coverage over the years.[15] I also divide my news into positive and negative news. A positive news report is considered to be adding a positive outlook for a firm. Increased dividends, increased buybacks, beating expectations, increased sales, acquisitions, mergers,[16] stakes, change to positive rating from neutral rating, and positive credit changes are examples of positive news. Negative news reports are considered to be giving

13 I find that mining is an industry always covered by breaking news in case of a privacy breach in my sample, but given the limited amount of observations, it may not be a trend in case of repeated breaches.

14 I want to control for the "permanent" media coverage of a given company, i.e. the average amount of news coverage a given firm gets. For example, JP Morgan Chase has on average more than 274.59 news articles a day in my sample, whereas Midas only has an average of 0.68 articles a day. Therefore an extra news article on a given day might have more effect on Midas than JP Morgan Chase.

15 I report all the results in the article using the year average as it takes into account the potential change in media coverage over time for a given firm.

16 Note that I only consider acquisitions as positive news events for acquired firms as acquirers tend to incur negative abnormal returns upon announcements. I also run a robustness check using all of mergers and acquisitions that led to an increase in abnormal returns after the announcement, using event studies. Withdrawn acquisitions are treated as negative news for the acquired (after event study analysis).

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

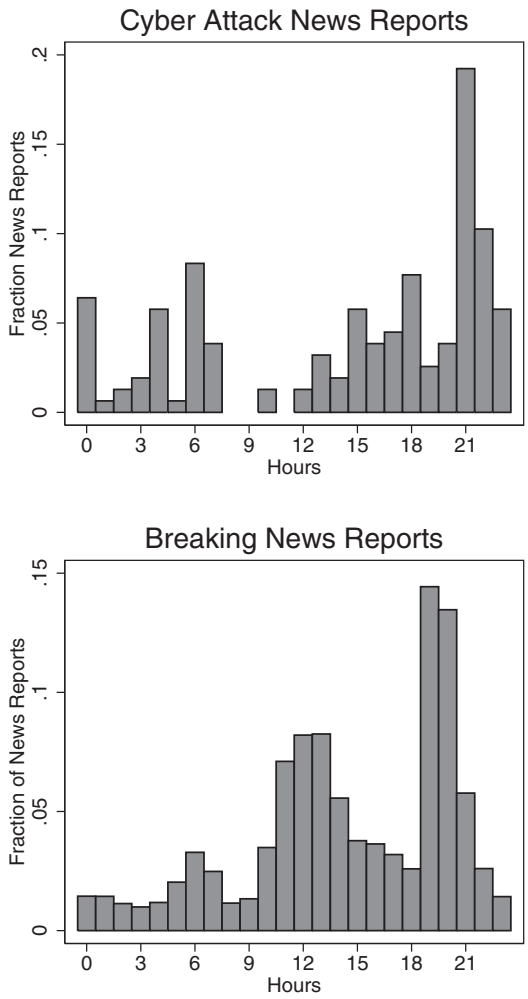

Figure 2: Distribution of news reports during the day.

a negative outlook on the firm. Examples of negative news include missed earnings, decreased sales, bankruptcy, product recalls, change to negative rating from neutral rating, and negative credit changes.[17] I construct $PABN_{it}$ "positive abnormal news reports" by measuring the amount of positive news reports compared to the "permanent" amount,

$$PABN_{it} = \frac{PN_{it} - \overline{PN_i}}{\overline{PN_i}}, \tag{2}$$

with PN_{it} the sum of positive news stories during day t for firm i and PN_i the average of the positive stories over the time period.

I also define $NABN_{it}$ "negative abnormal news reports" by measuring the amount of negative news reports compared to the "permanent" amount

$$NABN_{it} = \frac{NN_{it} - \overline{NN_i}}{\overline{NN_i}} \tag{3}$$

where NN_{it} is the sum of negative news stories during day t for firm i and $\overline{NN_i}$ represents the average of the negative stories over the time period.[18]

Fig. 1 plots the media coverage for the entire sample, dividing it into positive and negative news reports using the ratios in (2) and (3). Fig. 1 also contains the fraction of events that have a breaking news report on a given day around the privacy breach disclosure. I note that on average there are more breaking news reports after the breach disclosure, at least for the first few days. Moreover, there is a clear drop in average daily negative news compared to the permanent level around the breach disclosure. It has to be noted that the graph also contains all the negative news reports related to the breach, emphasizing that the small spike right after the breach is mainly due to the breach. Therefore, overall there is a significant decrease in abnormal negative news reports around the breach disclosure time. Firms seem to use a time when the firm does not have a lot of negative news reports to disclose a privacy breach. I also note that the daily abnormal positive news reports around the breach disclosure have a clear pattern. There is a large decrease in the amount of positive news compared to the permanent level prior to the breach and a strong increase right after the disclosure of the breach, at least for the first five trading days following the disclosure. It seems to show that firms decide to disclose the negative event of a privacy breach in a lower negative news environment and lower than usual positive news reports. Once the breach is disclosed, more positive news reports are released to the market. The proportion of breaking news reports around the breach disclosure is also interesting, as it shows that a breached firm will be more likely to have breaking news reports on average after release of a breach.[19] I also consider the press releases that firms issue around privacy breaches. I distinguish it from the other media as firms directly control press releases. Fig. 3 shows the average daily number of positive and negative press releases compared to the firms' average over the period, i.e. *P ABNit* and $NABN_{it}$. Prior to the breach, there is a significant drop in the number of negative press releases. Similar to the negative news reports, the negative press releases following the disclosure of the breach mainly relate to the breach. Therefore, it shows that negative press releases are actually down, when parsing out the privacy breach related press releases, over a period of around 10 trading days after the disclosure of a breach. Similarly, there are more positive press releases around the breach disclosure. I find a significant peak prior to the disclosure that may indicate that firms try to create a positive environment to ensure more positive news reports a few days before the disclosure. Similarly, there are more positive press releases on average right after the announcement. Overall, firms seem to create a positive environment around the breach disclosure time to ensure a lower negative impact on stock performance.

I consider how news coverage changes on the days around the breach disclosure. I also take into account the different state legal requirements about the timing of privacy breaches disclosures, which could explain why some firms are more likely to be in the news than others. Most states insist on the fact that there should not be any unreasonable delay for disclosing a privacy breach. In practice, the time period allowed for disclosure varies between 5 and

17 I also use as a robustness check for my results the sentiment analytics from the RavenPack dataset which examines each news reports based on story type, events, and tone. I choose five different sentiment scores that classify each news story as being either positive, negative, or neutral. My classification of the news is robust to those scores.

18 As previously mentioned, the averages are taken over different time periods for robustness check: average over the entire sample 2005–14 and average per year to better control to changes in company coverage over the years.

19 I also find in Fig. 2 that breaking news reports for firms are usually distributed during the day on average, but in the particular case of cyber-attacks breaking news reports the disclosure seems to happen mainly outside of the trading hours.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

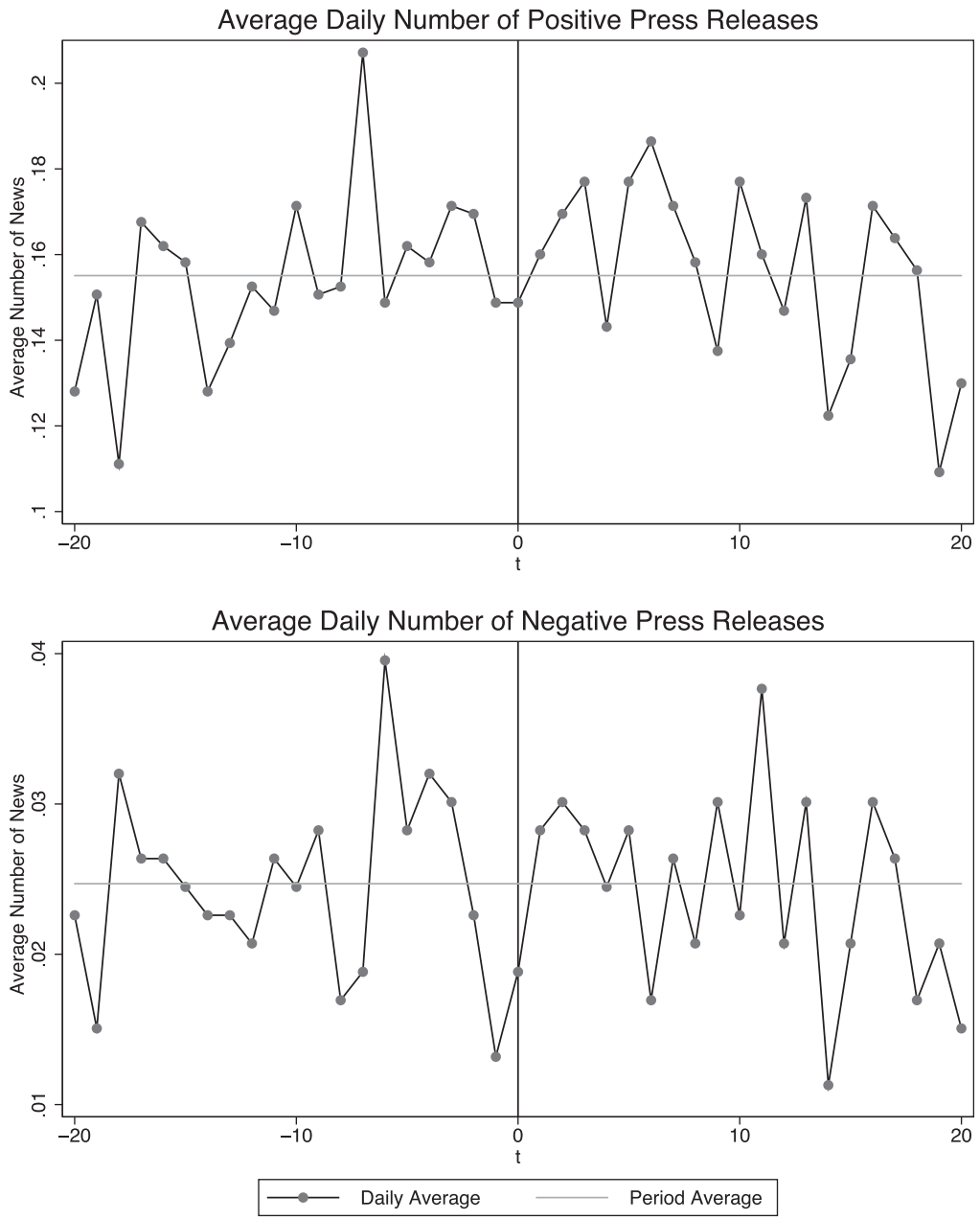

Figure 3: News reports directly released by firm.

90 days after discovery of the breach.[20] In states without disclosure laws, firms may wait longer to disclose the breach to their customers or the attorney general of the state.[21] I estimate the following equation for the positive news reports:

$$PN_{it} = \alpha + \beta X_{it} + \sum_{k=-l}^{l} \psi_k . PB_{i,t+k} + \sum_{j=-l}^{l} \phi_j . PB_{i,t+j} . DiscLaw_{i,t+j} \quad (4)$$

where X_{it} contains market capitalization, firms controls,[22] industry controls, year, month, and day controls. I cluster my regression at the firm level. $PB_{i,\ t+k}$ corresponds to the kth day after (if $k > 0$) or prior to the privacy breach disclosure at date t. Similarly, I run the following model for negative news reports:

$$NN_{it} = \alpha + \beta X_{it} + \sum_{k=-l}^{l} \psi_k . PB_{i,t+k} + \sum_{j=-l}^{l} \phi_j . PB_{i,t+j} . DiscLaw_{i,t+j}. \quad (5)$$

Table 5 shows the results of these regressions.[23] There is a significantly larger number of positive news reports on the day prior to the privacy breach disclosure, which is consistent with the fact that

20 As a reminder, I consider the date when the legislation was implemented in my empirical analysis. See, e.g. http://www.ncsl.org/research/telecommunications-and-information-technology/2014-security-breach-legislation.aspx. (23 May 2015, date last accessed).

21 For example, AT&T reported in June 2014 a breach on its customers' accounts that happened 2 months prior. See, e.g. http://www.cio.com/article/2369870/mobile/at-t-waits-a-month-to-notify-customers-of-data-breach.html) (30 March 2015, date last accessed).

22 As a reminder, firms control contains market capitalization, dividends, and market debt ratio.

23 I run the regressions with ψ_k or with ϕ_j terms for up to 10 days prior and after. I only report in Table 5 the results for $t = 1, 0, 1$ as the effect

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Table 5. Effects of privacy breaches on number of news events

	Number of positive categorized news	Number of negative categorized news	Number of positive categorized news	Number of negative categorized news	Number of positive categorized news	Number of negative categorized news
Privacy breach$_{t=-1}$	0.225*	0.0276			0.00504	−0.0964
	(0.122)	(0.0668)			(0.238)	(0.0911)
Privacy breach$_{t=0}$	−0.0278	−0.0981*			0.0860	0.111
	(0.113)	(0.0584)			(0.213)	(0.135)
Privacy breach$_{t=1}$	0.0634	0.0908			0.0410	−0.0973
	(0.101)	(0.0553)			(0.298)	(0.0942)
Disclosure law dummy × *privacy breach*$_{t=-1}$			0.288**	0.0635	0.283	0.160
			(0.145)	(0.0795)	(0.287)	(0.114)
Disclosure law dummy × *privacy breach*$_{t=0}$			−0.0609	−0.158**	−0.147	−0.269*
			(0.118)	(0.0663)	(0.216)	(0.155)
Disclosure law dummy × *privacy breach*$_{t=1}$			0.0697	0.145*	0.0288	0.242*
			(0.131)	(0.0761)	(0.365)	(0.141)
Market capitalization	0.108	0.0511	0.108	0.0511	0.108	0.0512
	(0.115)	(0.144)	(0.114)	(0.144)	(0.114)	(0.144)
Constant	1.789	1.279	1.796	1.280	1.793	1.282
	(1.649)	(2.095)	(1.648)	(2.094)	(1.649)	(2.092)
Firm controls	Yes	Yes	Yes	Yes	Yes	Yes
SIC industry controls	Yes	Yes	Yes	Yes	Yes	Yes
Year controls	Yes	Yes	Yes	Yes	Yes	Yes
Month controls	Yes	Yes	Yes	Yes	Yes	Yes
Day of week controls	Yes	Yes	Yes	Yes	Yes	Yes
N	32391	32391	32391	32391	32391	32391
R^2	0.359	0.317	0.359	0.318	0.359	0.318

Standard errors in parentheses.
*$P < 0.1$, **$P < 0.05$, ***$P < 0.01$.

firms tend to release a privacy breach disclosure in a more positive environment. More importantly, I find a significant and lower number of negative news reports on the day of disclosure, despite all the news related to the privacy breach. It tends to show that the firm avoids negative media environments around a breach disclosure. But for the breach disclosure both results seem to lead to an overall positive media sentiment about the firm.[24] When considering that those effects differ by state disclosure laws, I find that firms subject to disclosure laws tend to release significantly fewer negative news on the day of the announcement than firms without disclosure. This result is all the more important that it contains the news reports pertaining to the privacy breach. On the day after the announce ment, firms subject to the disclosure laws have more negative news reports mainly due to the privacy breach announcement itself. I also find that the day prior to the announcement firms subject to disclosure laws have a significantly larger amount of positive news compared to the other firms. This seems to point towards firms carefully picking a period when there are fewer negative news and more positive news reports to disclose the privacy breach.

Considering that the breach disclosure is a negative news event whose release is controlled by firms, I find that firms create an environment to alleviate its potential negative effect on the stock by bundling it with positive news around the time of disclosure (merger, patent, or joint venture).

In effect, firms build up a stock of positive and negative news that they release to the market when disclosing a privacy breach.[25]

In a way, the positive news reports act as an insurance payment for the stock of the company or a mechanism to increase noise about a firm to hide the negative privacy breach signal. Therefore, a firm has an incentive to keep some stock of positive news reports under wraps in case of a privacy breach. The stock price decrease due to the breach could then be offset by the timely release of positive news reports to the market on the same day. Also, the firm may want to avoid negative press releases to the market around the time of disclosure. We will analyze those effects in the next section.

News bundling and stock performance

So far, I presented evidence on timing of a privacy breach disclosure and positive media coverage environment. I consider in this section how this timing translates in terms of stock performance. I expect to find that firms will manage to lessen the negative effect on stock return of a privacy breach disclosure by bundling the announcement with some positive news reports. The effect for firms in states with disclosure laws should have a larger negative effect as they are more constrained than other firms in terms of timing of disclosure.

The amount of time between the breach and a news report disclosure varies from a few days up to 6 months. I consider breaking news reports on the day of the privacy breach announcement as the

of other days is insignificant. Most control variables are significant with *P*-values of 0.10. I use multiple comparison correction for the *P*-values as a robustness test.

24 The other days prior to or after the breach disclosure do not lead to any significant coefficient. I tested it using up to 10 days before and after as regressors.

25 If a privacy breach occurs, the company has to disclose it to the breached customers and the regulator (as well as the market) but has some leeway in its release. It may wait for a few weeks or months depending of state disclosures laws and the number of records breached.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Table 6. Effects of privacy breach reports

	(1) Ab.Returns Fama–French	(2) Ab.Returns Fama–French	(3) Ab.Returns Fama–French	(4) Ab.Returns Fama–French	(5) Ab.Returns Fama–French	(6) Ab.Returns Fama–French
Privacy breach$_{t=0}$	−0.271**	−0.270**				
Privacy breach$_{t=0,\,1}$	(0.133)	(0.133)	−0.245**	−0.244**		
Privacy breach$_{t=-1,\,0,\,1}$			(0.100)	(0.1000)	−0.259***	−0.259***
					(0.0849)	(0.0848)
Market capitalization		0.0191		0.0191		0.0191
		(0.0221)		(0.0221)		(0.0221)
Records breached > 100, 000	−0.00506	−0.00828	−0.0353	−0.0381	−0.0253	−0.0280
	(0.192)	(0.192)	(0.171)	(0.171)	(0.170)	(0.170)
Constant	0.158	−0.153	0.161	−0.150	0.167	−0.144
	(0.161)	(0.305)	(0.162)	(0.304)	(0.163)	(0.304)
SIC industry controls	Yes	Yes	Yes	Yes	Yes	Yes
Year controls	Yes	Yes	Yes	Yes	Yes	Yes
Day of week controls	Yes	Yes	Yes	Yes	Yes	Yes
N	16165	16165	16165	16165	16165	16165
R^2	0.001	0.001	0.001	0.001	0.0011	0.001

Standard errors in parentheses.
*$P < 0.1$, **$P < 0.05$, ***$P < 0.01$.

direct effect of the breach on a given firm valuation. This news release represents the moment when the market first learns about the breach and reacts to it. I will also look at the diffusion of the release of information of the breach on the stock behavior by analyzing both the short-run event studies approach and the panel data analysis of the announcement of the breaches. First, I perform event studies with windows of 10, 30, and 50 days prior and after the announcement. I then integrate the news bundle theory within the event studies to understand the pattern of news releases to the market on days of unexpected negative news release. In the panel data approach I examine the average effect of the breach on the adjusted value of firms, with the overall bundling of news coverage around the breach disclosure time. In this article, I report all of the results using a 30-day window around the disclosure.

Stock returns and privacy breach disclosures

I create a panel of privacy breaches and stock prices using for each firm data on news reports, breaking news, market capitalization, privacy breaches, and the number of records breached, for 30 trading days prior and after the breach disclosure.

I first consider the immediate short-run impact of a privacy breach to the value of a company considering both 10 and 50 trading days before and after the event. I restrict the sample of privacy breaches used in the event studies to include stocks with a full span of 10 days or 50 days of trading around the breach date. I disregard stocks breached right after their IPOs or at the end of my sample to avoid any unexpected results due to the IPO and the lack of data post breach. I included those stocks later for robustness checks. I generate the abnormal returns *ARit* for each firm and period using the Fama–French controls to account for market fluctuations, using the historical prices for 10 and 50 days before the disclosure events. I chose to consider whether breaches affected more than 100 000 records. This number is seen in the privacy industry as the cutoff for a large breach.

I estimate the direct effect of a privacy breach disclosure using the following equation:

$$AR_{it} = \zeta + \theta X_{it} + \lambda Privacy\,Breach_{it} + \varepsilon_{it} \quad (6)$$

where *Privacy Breachit* is a dummy if there is a breach disclosure on day *t* for firm *i*. The controls X_{it} contain the following variables: (log of) market capitalization, number of records breached (when available), industry controls, year controls, and days of the week controls for each firm *i* and day *t*. I also run the regression adjusting *Privacy Breachit* for a disclosure on the day or the day after. In this case, the dummy takes the value of 1 on both the day and day after the disclosure. I use firm-level, SIC-level and multi-level using SIC and day clustering in my analysis [31]. When multiple firms are part of a same breach, I also cluster at that particular group level as a robustness check to control for potential within industry dependence. I used clusters on industries and robust standard errors for robustness checks. The results are unchanged. I also considered a non-parametric inference approach to individual level event studies [32, 33].

Table 6 reports the results of this regression. I find that there is a significant negative effect of a breach disclosure (−0.27%) on the day and the next (−0.24%). I notice that the market capitalization and the number of records breached are not significant. It may be due to the fact that records are only a by-product of a breach and investors are more concerned about the fact that the firm itself was breached. In specification (6), I report a significant −0.25% effect on the abnormal returns if there is a privacy breach dummy disclosure on the day, or the day before or after disclosure.[26] All of the results are robust to the choice of specification and controls. I show in Fig. 4 the average abnormal returns and average cumulative abnormal returns for the firms in my sample. I find that there is on average a negative abnormal return over the 30-day trading period after the privacy breach disclosure. I notice that if I control for news reports the shape of the average abnormal returns are similar, but

26 As a reminder, a breaking news report about the breach on the day prior to disclosure means that the disclosure happened after hours on the previous trading day.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

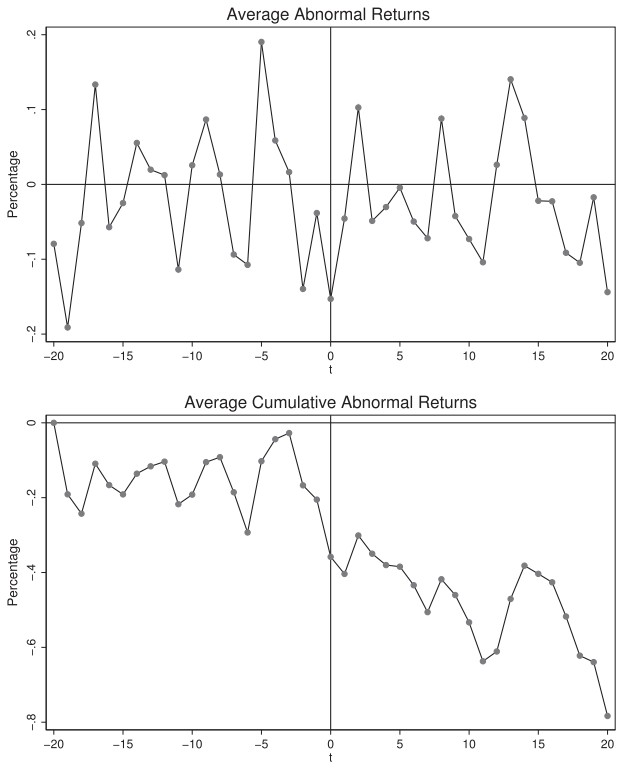

Figure 4: Average firm returns.

the negative abnormal returns are most of the time less negative than when not controlling for the news. I also see that the average cumulative abnormal returns is mainly decreasing over the 30 days around the breach.[27] Those patterns are different for every firm in the sample. Almost half of the firms actually see positive abnormal returns after the disclosure of the privacy breach.[28] This type of different behavior might be due to the timing of the disclosure. Given the pattern found on the positive and negative news reports, firms seem to use positive news reports as a way to insure themselves against a larger drop in stock price.

In order to check this result, I modify Equation (6) to incorporate the news report effects as follows:

$$\begin{aligned} AR_{it} = \zeta + \theta X_{it} + \alpha_1 BR_{it} + \alpha_2 BR_{it}.D_{it} \\ + \gamma_P PABN_{it} + \gamma_{P0} PABN_{it}.D_{it} \\ + \gamma_N NABN_{it} + \gamma_{N0} NABN_{it}.D_{it} + \varepsilon_{it} \end{aligned} \quad (7)$$

X_{it} contains all of the other controls for the regression: market capitalization, SIC industry controls, year controls, day of the week controls, and Fama–French factors. BR_{it} is a dummy for breaking news on day t for firm i. D_{it} is a dummy variable of the privacy breach disclosure for firm i at date t that is equal to 1 at date t of the disclosure for firm i. The variable $BR_{it}.D_{it}$ represents the presence of a breaking news report on the privacy breach disclosure on the disclosure day. The variables $NABN_{it}.D_{it}$ and $PABN_{it}.D_{it}$ represent negative and positive abnormal news reports, respectively, on the day of disclosure of the privacy breach (also called positive and negative news ratio, respectively).[29] Table 7 presents the results of this regression. I find that overall abnormal returns on the day of disclosure are significantly and positively affected by abnormal positive news reports on average. I still find that on the day of disclosure of a privacy breach, a breaking news report leads to a significant negative effect of −0.25% on the abnormal returns, controlling for any abnormal amount of news. On any other day breaking news reports actually have no significant effect or are more likely to have a small but positive effect on the stock price. I find that the effect of abnormal positive news reports is significant and large (0.46%). It is 15 times higher than the effect on any other day (0.03% and significant) and therefore offsets the potential negative effect of the privacy breach disclosure. This large effect may be partly due to the more positive environment created by the firm right before releasing the disclosure about the breach as seen in the earlier figures. Investors might be more receptive to good news on days when expectations are lower due to an unexpected negative breaking news report. On the contrary, abnormal negative news reports have usually a significant but small negative effect (−0.03%). But on the day of a privacy breach disclosure this effect is small, positive, and most of the time insignificant. It implies that firms may release some other negative, but less strategic negative news that the market puts into perspective with the privacy breach. In sum, it explains why stocks could increase on the day of a disclosure of a privacy breach and raises the question of the effects of bundling news by companies as the firm likely has the power to counteract the negative effect of the privacy breach disclosure by providing one additional unit of positive abnormal news.[30] I also find that stocks of firms with a larger market capitalizations are also significantly lower due to the privacy breach disclosure. It could mean that larger firms need to release more positive information to alleviate the negative effect of a disclosure of a breach.

I also examine if the effects of privacy breach disclosures differ by type of industry, given that news coverage varies per industry.[31] Table 8 shows that privacy breaches in the banking or insurance industry reported with a breaking news report lead to a large, significant negative effect on the stock price due mainly to the sensitive customer data they own. Similarly, there is a large, negative significant effect of a privacy breach announced through a breaking news report for the wholesale trade and services industries. It may be due to the fact that transaction costs for consumers to switch between those firms is small contrary to the financial industry. Therefore, if a privacy breach occurs and customer data has been compromised, investors anticipate a switch to another provider of goods.[32]

27 The dataset for events studies are a subset of my large panel dataset. I only consider privacy breach events that are only separated by 30 days to avoid any cofounding effects.

28 Overall 57.5% of my sample leads to negative abnormal returns on the day of disclosure of a privacy breach. Using news controls, years, days of the week, industry, I find that the negative abnormal returns drop to 54.4% of my sample.

29 I also add the type of privacy breach (hacking, laptop stolen) and the type of data that was stolen. The types of data stolen are social security number, names, credit card. I find that controlling for the changes in news changes the impact on the abnormal returns, but overall does not alter the signs of the abnormal returns of the stock. Surprisingly, the different types of breaches do not have a significant effect on the returns.

30 There could be a strategy for the firm to disclose around the same time some minor negative news that it has to disclose by law. In some specifications, the negative news reports actually have a very small and significant effect.

31 I control those effects per industry using positive and negative news per division and firm. The standard errors are clustered at the industry and firm level. Results in the article are reported at the firm level.

32 A privacy breach is as likely to affect any company within the industry. If one of them gets breached, the entire industry as a whole does not necessarily benefit: firms in the industry need to upgrade their defenses to avoid becoming the next target of a breach.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Table 7. Effects of news events and privacy breach reports

	(1) Ri − rf	(2) Ri − rf	(3) Ri − rf	(4) Ri − rf	(5) Ri − rf	(6) Ri − rf
Breaking news	−0.00806	0.134***	0.0291	−0.00791	0.135***	0.0292
	(0.0244)	(0.0261)	(0.0249)	(0.0244)	(0.0261)	(0.0249)
Breaking news$_{t=0}$	−0.240**	−0.0473	−0.249**			
	(0.101)	(0.192)	(0.101)			
Breaking news$_{t=0,\,1}$				−0.189**	−0.0909	−0.188**
				(0.0872)	(0.121)	(0.0875)
Positive news ratio	0.0358***		0.0433***	0.0358***		0.0433***
	(0.00312)		(0.00336)	(0.00312)		(0.00336)
Negative news ratio		−0.0284***	−0.0332***		−0.0284***	−0.0332***
		(0.00256)	(0.00275)		(0.00256)	(0.00275)
Positive news ratio$_{t=0}$	0.467***		0.460***	0.466***		0.459***
	(0.129)		(0.129)	(0.130)		(0.130)
Negative news ratio$_{t=0}$		0.0373*****	0.0164		0.0375***	0.0162
		(0.0104)	(0.0165)		(0.0103)	(0.0166)
Market capitalization	−0.210***	−0.214***	−0.211***	−0.210***	−0.214***	−0.211***
	(0.0648)	(0.0650)	(0.0650)	(0.0648)	(0.0650)	(0.0650)
Constant	3.495***	3.428***	3.499***	3.495***	3.428***	3.499***
SIC industry controls	Yes	Yes	Yes	Yes	Yes	Yes
Year controls	Yes	Yes	Yes	Yes	Yes	Yes
Day of week controls	Yes	Yes	Yes	Yes	Yes	Yes
Fama–French controls	Yes	Yes	Yes	Yes	Yes	Yes
N	529591	528226	528226	529591	528226	528226
R^2	0.128	0.128	0.129	0.128	0.128	0.129

Standard errors in parentheses.
*P <0.1, **P < 0.05, ***P < 0.01.

Table 8. Effects of news events and privacy breach reports on the panel by SIC industry division

	(1) Ab.Returns Fama–French	(2) Ab.Returns Fama–French	(3) Ab.Returns Fama–French
Construction × *breaking news*$_{t=0}$	−0.985		
	(0.614)		
Mining × *breaking news*$_{t=0}$	−0.190	−1.890	0
	(0.675)	(0.674)	
Manufacturing × *breaking news*$_{t=0}$	0.0496	0.040	0.008
	(0.289)	(0.289)	(0.290)
Transportation, communication, electric, gas and sanitary services × *breaking news*$_{t=0}$	−0.316	−0.317	−0.206
	(0.352)	(0.351)	(0.341)
Wholesale Trade × *breaking news*$_{t=0}$	−1.035***	−1.060***	−1.244*
	(0.226)	(0.226)	(0.666)
Retail Trade × *breaking news*$_{t=0}$	−0.665*	−0.677*	−0.353
	(0.360)	(0.360)	(0.265)
Finance, insurance and real estate × *breaking news*$_{t=0}$	−0.549**	−0.557***	−0.348**
	(0.215)	(0.215)	(0.177)
Services × *breaking news*$_{t=0}$	−0.869*	−0.877*	−0.494*
	(0.467)	(0.466)	(0.274)
Other × *breaking news*$_{t=0}$	−0.273	−0.269	−7.11
	(0.377)	(0.377)	(8.407)
Abnormal positive news	Yes	Yes	No
Abnormal negative news	Yes	Yes	No
Abnormal positive news × division	No	No	Yes
Abnormal negative news × division	No	No	Yes
Market capitalization	Yes	Yes	Yes
Year controls	Yes	Yes	Yes
Day of week controls	Yes	Yes	Yes
Observations	530	528	528
R^2	0.486	0.486	0.589

Standard errors in parentheses.
*P < 0.1, **P < 0.05, ***P < 0.01.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Overall, I find that privacy breaches announcements have a negative effect on the stock prices of companies, but this effect is short-lived.[33] Privacy breaches are random events that shock the stock of the firms as a surprise announcement, but in the long run should not have a large effect as firms have insurance, engage in public relations strategy, and increase their level of security for the future. Media coverage plays a central role in determining the performance of firms' stocks around privacy breach disclosures. Disclosing in a period with a largely positive media environment leads to a smaller negative effect on the stock performance. This result complements the previous section where I showed that firms strategically manage the news flow around the disclosure of privacy breaches. In this section, I presented evidence that this concerted media effort has an effect the firm's stock performance.

Overall, firms follow the following process: they first choose to disclose a privacy breach during a more positive media environment, within the legal requirements in states with disclosure laws. Then they may also look to add to positive news reports on or around the disclosure by announcing more positive events, like joint ventures, raised guidances. Given the positive market environment generated by those positive news reports, other negative news may have a lower effect on the stock of the company. It could be a window to release less important negative events to the market, as most of the media coverage would be centered on the privacy breach.[34]

Disclosure laws and portfolios

In this section, I analyze the effect of state disclosure laws on stock returns of breached firms. I found in Table 5 that news coverage is affected by the different type of disclosures. Previous results suggest that firms find it harder to control the negative effect of a privacy breach using a more favorable environment. I want to measure whether states with disclosure laws can effectively incentivize firms to improve their data security and limit the effect of a privacy breach on the misuse of consumers' sensitive information. In those states, firms have to report the existence of a breach and its full impact to customers and the state attorney general in a timely manner. The goal of this practice is to prevent a misuse of the personal customer data.

Simply put, data breach disclosure laws require firms to notify breach-affected individuals within a reasonable timeframe, no later than 45 calendar days[35] after discovery of the breach. The breach is considered "discovered" on the first day it is known (or reasonably should have been known) by a breached firm.

I consider a variation of the previous model adding the disclosure laws by states as follows:

$$AR_{it} = \zeta + \theta M_{it} + \varphi DL_{it} + \phi_p DL_{ip}.d_{i,p} + \ldots + \phi_5 DL_{it}.d_{i,p+5} + \varepsilon_{it} \quad (8)$$

where *Mit* corresponds to all of the controls in Equation (7). The disclosure laws are *DLit* for state *i* at time *t*. I also consider their impact on each particular trading day after the disclosure using the potential breaking news about the data breach *dip* where *p* is the day of the privacy law disclosure. The terms *DLit.dip* represent the effect of a breaking news on the day of the disclosure of the privacy breach in a state with *DLit* disclosure law. Table 9 reports the results of the estimation.

I find that controlling for states and number of records breached, disclosure laws by states have a negative and significant effect on the returns (−0.17%) but this effect is significant when including the breaking news reports. It may be due to the fact that if firms have to disclose privacy breaches they may only partially control the timing of the disclosures themselves. In the case of breaches occurring in states without disclosure laws, firms might feel confident to release the news to the market as a sign of strength in their ability to handle the crisis and solve the problem.[36] I also notice that on the day before the disclosure abnormal negative news reports have a stronger negative effect than usual on the returns in states with disclosure laws, about 9 times larger than usual. Alternatively, abnormal positive news reports have a strong positive effect of smaller magnitude (only 3 to 4 times larger than in Table 7).

I also estimate that a company that disclosed a breach in a state with disclosure laws has a negative and significant effect on the abnormal returns of its stock on the day after the disclosure (−0.70%) when a breaking news report is issued about it the day after the breach.[37] This significant result actually helps an investor as they could short a breached firm or buy an option on the stock on the day after the disclosure of the breach as soon as a breaking news report is released. I consider buying a $1 of the stock of a firm that was breached on the day after disclosure and selling it at the end of the day over the entire time period 2007−14. I compare this portfolio to a simple portfolio consisting in buying $1 of a weighted (by market capitalization) average index of the three main stock exchanges in the USA (NASDAQ, NYSE, and AMEX).[38] Fig. 5 shows the "breached firms" portfolio and the composite index over the period 2007−14.[39]

33 This is why a given stock may react positively or negatively to a disclosure of a privacy breach based on the mix of news on or around the day of the disclosure: if I suppose that firms choose to disclose privacy breaches at the same time as other news reports, the news reports will actually affect the returns of the stock. It may depend on what investors will weigh more in their stock analysis.

34 Given that positive news reports are strategically released to the market, the number of records breached should have a very small effect on the abnormal returns of the stock on the day of the breach disclosure.

35 This timeframe depends on the type of breach and the state where the breach occurred. Most states require firms to send notices to affected customers with a brief description of the breach, including (if known) the date of the breach and the date of the discovery of the breach; the information stolen; procedure for affected customers to protect themselves from potential harm as a result of the breach; updates on investigation of the breach and future protection against any further breaches; and contact information.

36 I run the analysis both with and without state dummies as the disclosure laws are state-specific.

37 I find that this effect is only significant for the day after the disclosure and disappears as soon as the second day. I also find that controlling for disclosure state laws the negative news other than the breaches seems to significantly slightly increase the returns of the stocks.

38 Using an S&P500 index leads to similar results.

39 Comparing the returns by year over my full period 2005–14 leads to 2007 and the period 2009–14 outperformance of the market. This is due to the fact that contrary to the 2005–06 trading period, investors have adapted to the idea of a breach as a transitory, unavoidable shock. Similarly, given the effect of breaking news of privacy breach in states with disclosure laws, I short the breached stocks over the day and found that the strategy would outperform the index in 2006, 2008, 2011, and 2013.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Table 9. Effects of media coverage, privacy breaches, and disclosure laws

	(1) Ab.Returns Fama–French	(2) Ab.Returns Fama–French	(3) Ab.Returns Fama–French	(4) Ab.Returns Fama–French
Breaking news	−0.0221	−0.0132	−0.0219	−0.0405
	(0.0392)	(0.0270)	(0.0391)	(0.0386)
Breaking news$_{t=-1}$	−0.0980	0.808	−0.0979	−0.0839
	(0.314)	(0.629)	(0.314)	(0.319)
Breaking news$_{t=0}$	−0.508**	−0.506**	−0.541**	−0.474*
	(0.237)	(0.234)	(0.216)	(0.245)
Breaking news$_{t=1}$	0.261	0.118	0.261	0.252
	(0.244)	(0.198)	(0.244)	(0.239)
Positive news ratio	0.0155	0.0308***	0.0155	0.0120
	(0.0135)	(0.0107)	(0.0135)	(0.0130)
Positive news ratio$_{t=-1}$	−0.0308	−0.106***	−0.0309	−0.0231
	(0.0331)	(0.0325)	(0.0331)	(0.0338)
Positive news ratio$_{t=0}$	0.167*	0.462***	0.168*	0.170*
	(0.0988)	(0.134)	(0.0982)	(0.0982)
Positive news ratio$_{t=1}$	−0.0916	−0.0439	−0.0916	−0.0887
	(0.0766)	(0.0492)	(0.0766)	(0.0772)
Negative news ratio	−0.0392***	−0.0367***	−0.0392***	−0.0335***
	(0.0111)	(0.00804)	(0.0111)	(0.0101)
Negative news ratio$_{t=-1}$	−0.271*	−0.0675	−0.271*	−0.276*
	(0.140)	(0.102)	(0.140)	(0.141)
Negative news ratio$_{t=0}$	0.0437***	0.0193	0.0431***	0.0385***
	(0.0136)	(0.0174)	(0.0132)	(0.0128)
Negative news ratio$_{t=1}$	−0.0205	0.0342	−0.0205	−0.0257
	(0.0692)	(0.0343)	(0.0692)	(0.0686)
Market capitalization	0.0271	0.00219	0.0270	0.0530^{+}
	(0.0232)	(0.0102)	(0.0232)	(0.0323)
Disclosure law dummy	−0.0229	−0.0379	−0.0230	−0.169*
	(0.0631)	(0.0504)	(0.0631)	(0.0950)
Disclosure law dummy × *breaking news*$_{t=-1}$	−0.210	−0.870	−0.210	−0.228
	(0.422)	(0.656)	(0.422)	(0.427)
Disclosure law dummy × *breaking news*$_{t=0}$	0.259	0.264	0.276	0.221
	(0.262)	(0.253)	(0.259)	(0.271)
Disclosure law dummy × *breaking news*$_{t=1}$	−0.704**	−0.328^{+}	−0.704**	−0.701**
	(0.307)	(0.214)	(0.307)	(0.303)
Records breached > 100 000	−0.0747			−0.0907
	(0.182)			(0.186)
Constant	−0.272	0.404*	−0.272	−1.273*
	(0.313)	(0.214)	(0.313)	(0.693)
SIC industry controls	Yes	Yes	Yes	Yes
Year controls	Yes	Yes	Yes	Yes
Day of week controls	Yes	Yes	Yes	Yes
State controls	No	No	No	Yes
N	16104	32330	16104	16043
*R*2	0.003	0.004	0.003	0.003

Standard errors in parentheses.
$^{+}P < 0.15$, $*P < 0.1$, $**P < 0.05$, $***P < 0.01$

I find that in states with disclosure laws and without breaking news reports, the portfolio hugely outperforms the index, 60 versus 20. The portfolios without both disclosure laws and breaking news reports lead to a smaller return, but might still outperform the index. In states without disclosure laws and breaches are reported by breaking news reports, the portfolio would also outperform the index. It may be due to the fact that firms report a breach, while not required to do so, leading investors to sell shares out of concern for a larger breach. Buying those stocks in the portfolio results in using the volatility of the stock on those days. When breaches are reported through a breaking news report and firms required to report a privacy breach in states with disclosure laws, the portfolio leads to a worse return than the composite index.[40]

Stock returns and type of breach

I explore how my analysis of privacy breach disclosures compares to other uncontrolled negative news events for the firms in my sample

40 As a reminder, I construct my portfolio buying a dollar of a stock of a firm disclosing a breach on day t compared to buying a dollar of the composite index on the same day t. I sell both those "stocks" at the closing price of the next day ($t+1$). Therefore, the index performance is different on days whether firms with or without disclosure laws are breached.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

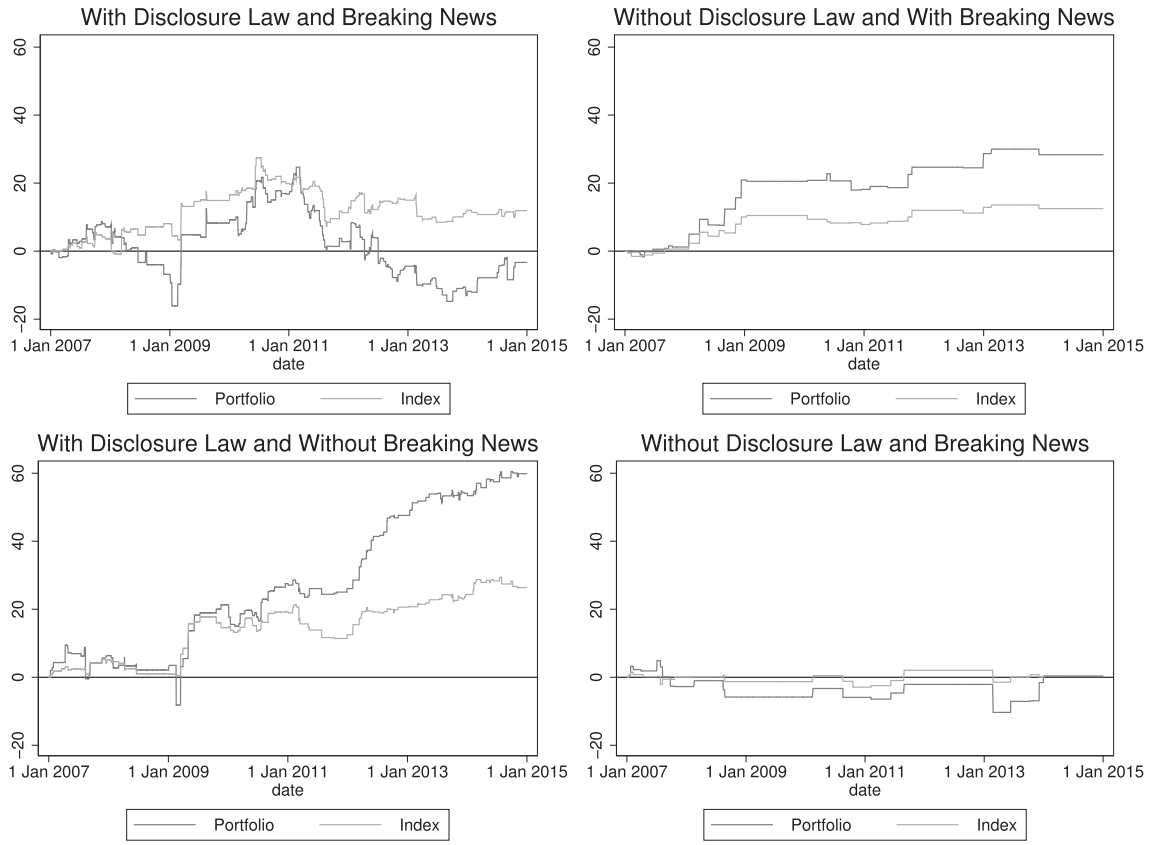

Figure 5: Portfolio construction.

Table 10. Comparison of reported news events

	(1) Privacy breaches	(2) Cyber-attacks	(3) Analyst rating downgrade	(4) Congressional hearing	(5) Copyright infringement	(6) Fraud	(7) Industrial accidents	(8) Lawsuits	(9) Patent infringement	(10) Product recall
Event reported$_{t=0}$	−0.270**	−0.530**	−1.425***	−0.211	1.029	−0.618	0.177	−0.0759	0.0772	0.0772
	(0.133)	(0.246)	(0.119)	(0.231)	(0.906)	(0.480)	(0.201)	(0.0632)	(0.112)	(0.133)
Market capitalization	0.0191	0.0424	−0.00245	0.0350	−0.0263***	0.301	0.0312	−0.0194	−0.0255	−0.0120
	(0.0221)	(0.0934)	(0.00586)	(0.0250)	(0.00560)	(0.356)	(0.0262)	(0.0127)	(0.0169)	(0.0135)
Constant	−0.153	1.063	0.203**	−0.388	0.804**	−6.219	−0.546	0.349*	0.662*	0.194
	(0.305)	(0.997)	(0.0941)	(0.598)	(0.342)	(7.089)	(0.462)	(0.179)	(0.339)	(0.266)
SIC industry controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Day of week controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	16165	3294	330678	1769	610	2928	5795	157134	9211	17934
R^2	0.0001	0.007	0.003	0.008	0.052	0.004	0.012	0.000	0.004	0.004

Standard errors in parentheses.
*$P<0.1$, **$P<0.05$, ***$P<0.01$.

to compare the effect of the breach to the other events over 2005–14. I consider nine other types of events: cyber-attacks, analyst rating downgrades, congressional hearings, copyright infringement claims, fraud, industrial accidents, lawsuits, patent infringement, and product recalls.[41] I consider the same regression as above to find the effect of breaking news on the day of disclosure of each particular event:

$$AR_{it} = \zeta + \theta X_{it} + \lambda Event_{it} + \varepsilon_{it}, \quad (9)$$

where *Eventit* is a dummy if there is an event disclosure on day *t* for firm *i*.

Table 10 reports the results on only the effect of the day of disclosure. A breaking news report on the day of disclosure of cyber-attacks, a subsample of my overall sample of privacy breaches, has a significant negative effect on the abnormal returns. The coefficient for cyber-attacks is twice the coefficient for privacy breaches in general (−0.53% versus −0.27%). I find that

41 I use the same method outlined in the empirical strategy section of the article to calculate the abnormal returns.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

Table 11. Comparison of reported news events

	(1) Privacy breaches	(2) Cyber-attacks	(3) Analyst rating downgrade	(4) Congressional hearing	(5) Copyright infringement	(6) Fraud	(7) Industrial accidents	(8) Lawsuits	(9) Patent infringement	(10) Product recall
Breaking news	−0.0141	−0.0872	−0.0204	−0.173	0.229	−0.119	0.0606	0.0263	−0.0361	0.00672
	(0.0238)	(0.154)	(0.0134)	(0.186)	(0.285)	(0.174)	(0.0414)	(0.0313)	(0.0468)	(0.0396)
Breaking news$_{t=0}$	−0.291***	−0.509	−0.614***	−0.571**	0.252	−0.281	−0.0748	−0.0698	0.109	−0.208
	(0.108)	(0.430)	(0.0928)	(0.222)	(0.595)	(0.556)	(0.154)	(0.0754)	(0.167)	(0.144)
Positive news ratio	0.0300***	0.0838**	0.0487***	0.0829	0.0197	0.0349	0.0386	0.0485***	0.0935***	0.0333*
	(0.009)	(0.0406)	(0.00816)	(0.0586)	(0.0815)	(0.0780)	(0.0234)	(0.00731)	(0.0228)	(0.0167)
Negative news ratio	−0.0366***	−0.0563	−0.0437***	−0.0225	0.0668	−0.0631	−0.0211	−0.0452***	−0.0646***	−0.0643***
	(0.007)	(0.0342)	(0.00439)	(0.0408)	(0.200)	(0.0612)	(0.0131)	(0.00530)	(0.0211)	(0.0161)
Positive news ratio$_{t=0}$	0.464***	0.260**	−0.0889***	−0.168	−0.496	−0.169	−0.0662	−0.0416	−0.0178	−0.0546**
	(0.134)	(0.125)	(0.0252)	(0.143)	(0.358)	(0.330)	(0.116)	(0.0341)	(0.0593)	(0.0242)
Negative news ratio$_{t=0}$	0.0179	0.0572*	−0.0561***	0.142***	0.141	−0.000191	0.0509	0.0423***	0.0650**	0.0995***
	(0.0177)	(0.0295)	(0.0119)	(0.0493)	(0.261)	(0.0871)	(0.0326)	(0.00657)	(0.0249)	(0.0293)
Market capitalization	0.00128	0.0448	−0.00274	0.0266	−0.0272***	0.304	0.0263	−0.0221	−0.0225	−0.0113
	(0.0103)	(0.102)	(0.00597)	(0.0220)	(0.00659)	(0.360)	(0.0269)	(0.0154)	(0.0191)	(0.0148)
Constant	0.456**	1.072	0.207**	−0.0472	0.708*	−6.174	−0.493	0.406*	0.632*	0.153
	(0.196)	(0.963)	(0.0941)	(0.528)	(0.318)	(7.124)	(0.481)	(0.206)	(0.355)	(0.276)
SIC industry controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Day of week controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	32330	3294	330674	1769	610	2928	5795	157134	9211	17934
R	0.003	0.007	0.0010	0.0016	0.063	0.004	0.016	0.002	0.018	0.017

Standard errors in parentheses.
$^{*}P<0.1$, $^{**}P<0.05$, $^{***}P<0.01$.

disclosure of an analyst downgrade through breaking news reports has also a strong negative effect on the abnormal returns (−1.42%). Other categories do not seem to respond significantly to the breaking news reports, but the effects might be due to a small number of observations. It may be due to the fact that lawsuits, industrial accidents, fraud, copyright infringement claims, patent infringement, and product recalls are not as well-defined events in the news reports.

I consider the same regression to get the effect of the disclosure of the event by breaking news, as well as positive and negative news reports:

$$\begin{aligned} AR_{it} = {} & \zeta + \theta X_{it} + \alpha_1 BR_{it} + \alpha_2 BR_{it}.D_{it} \\ & + \gamma_P PABN_{it} + \gamma_{P0} PABN_{it}.D_{it} \\ & + \gamma_N NABN_{it} + \gamma_{N0} NABN_{it}.D_{it} + \varepsilon_{it}, \end{aligned} \tag{10}$$

where D_{it} corresponds to the day of the disclosure of the considered event.

The results for Equation (10) with positive and negative news reports are in Table 11. I find that, when controlling for positive and negative abnormal news reports, both on the day of disclosure and other days, the effect of the breaking news reports on the day of disclosure on the abnormal of returns disappears for most of the different events. Most of the relevant information on the cyber-attacks might be concentrated in the type of abnormal news on the day of disclosure, positive or negative. The analyst downgrade event breaking news still has a negative, significant effect (−0.61%) but seems to have a negative externality on all types of news on the day (both coefficients on positive and negative abnormal news reports are negative). Congressional hearings breaking news reports have a negative and significant effect (−0.57%) when controlling for news reports. These results suggest that privacy breaches are a different type of event than the nine mentioned above (except for cyber-attacks). They are more random and firms have no control on whether or not a breach happens, even if they take appropriate measures for security.

Discussion

In this article, I showed that the overall effect of privacy breach disclosure was, on average, small and significant. As random events affecting firms only a few times over their lifetime, privacy breaches are short-term mitigated relevant events. Privacy breaches have a long-run effect of −0.24% on the value of the firm if I use only the day the breach was disclosed. If I extend the window to both the day and the day after the breach, the result is still robust at −0.18%. The result is also robust to different specifications using year, trading days, and industry controls. Overall, the impact of privacy breach disclosures on the value of firms is small, reinforcing that financial markets are efficient due to the low and corrected effect over time. It may reveal that firms take advantage of the decreased expectations of the stock returns on the breach disclosure day to unload positive news onto the stock. This would lead to a positive bounce in the stock value. Firms may also use the breach as an opportunity to hide some other negative news on the day of the disclosure. I indeed evaluate that negative news on that day has mainly an insignificant effect on the stock price, contrary to the significant and negative effect of negative news on other days. Privacy breach disclosure days may be a strategic time to release to the market some negative news while investors are focused on both the privacy breach and the positive news reports released.

My empirical results are in line with recent attempts in the literature that find that security events occurring in more recent years have less significant impact than earlier ones [34]. Given that breaches are random events and that they affect firms only a few times over their lifetime, I can think of them as mitigated relevant events. It is a clear decrease from (−0.58%) from 2000–05 found in

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

earlier papers relying on smaller samples [8, 24, 26].[42] Another explanation for the small effect of privacy breach disclosure on the market is the consumers' breach fatigue. Also, I may consider that the decline in response over the years to a given privacy breach might be due to the number of privacy events overall: Acquisti *et al.* counts only 79 events compared to my 501 over 8 years (both studies only counting events concerning companies traded on the stock market) [8].

I prove that in the short run the stock price of breached firms can increase, decrease, or stay stable as a result of a privacy breach disclosure, controlling for other market factors. Contrary to other events affecting a company, privacy breaches are somewhat expected by investors due to the randomness of the event and the lack of clear determination on how privacy breaches happen. This result should be compared to other potential events affecting companies: Jarrell and Peltzman use auto recall announcements and find a significant decrease in share prices between 2.5% and 3.5%, Dowdell *et al.* find a decrease of 29% of Johnson and Johnson stock after the 1982 tainted Tylenol episode was revealed, and Jory *et al.* find that corporate scandals decrease share prices between 6.5% and 9.5% within the first month after the announcement [35–37]. These studies were using events that were widely unexpected at the time and might have provided large effects. They also do not control for news reports around the date of the announcement.

My results suggest that the effects of a privacy breach on a breached firm are very small, but significant. I also find that an abnormal number of positive news on the day of disclosure helps offset a decrease of abnormal returns due to the disclosure of a privacy breach. There are multiple public policy implications to my results. First, given that there is a significant negative but small effect of the news reporting of a breach, imposing a press release reporting for all types of breaches would lead to more transparency. This is a larger-scale reporting than simply notifying breached customers as per security breach laws. Such a new policy has a small cost on the firm at the time of release but leads to faster and transparent breach reporting. Also, if a firm fears that a larger breach would have a larger negative effect on its reputation, and in turn on its stock, it would be incentivized to protect its data better against any privacy breach. The added weight of facing instantly the market reaction and public judgment should lead companies to increase their security practices.

Second, the result on news provides a strategy for firms to protect themselves against a negative, random, unexpected disclosure. Firms need a stock of positive news reports to outweigh the potential negative effect of the unexpected disclosure. Using my comparisons with other negative and unexpected events I notice that this method would only work for (cyber-attacks and) privacy breaches.

Third, the portfolios on firms disclosing privacy breaches constructed in section "News bundling and stock performance" show that firms subject to disclosure laws and breaking news reports experience a decrease in stock price. It may be a source of punishment for firms if they are not compliant with a growing need for private data security.

Conclusion

This article analyzes the effects of privacy breach disclosures and its potential bundling with positive news on that day on the stock market. My key finding is that firms manage to avoid the full negative effect of a privacy breach event disclosure by releasing on the same day an abnormal amount of positive news to the market. Specifically, I show that after the "breaking news" release of a privacy breach a large amount of positive news to the market tends to have a dominating effect. My results suggest that a larger abnormal amount of positive news on the day of the breach disclosure more than offsets the negative effect of the disclosure. These findings are consistent with the empirical behavioral literature where bad news reports are usually released to the market when investors are not paying attention. In my particular case of privacy breaches, investors are distracted by the negative news report on privacy breaches. I provide evidence that firms tend to release bundled news to the market to offset negative random events, potentially stocking good news. Contrary to planned news that firms prepare months in advance, most privacy breaches need to be disclosed within 2 months of discovery. I find that there exists a strategic bundling of news by firms around unexpected negative events. My interpretation focuses on the premise that firms are not entirely in control of a privacy breach release and will try to bundle positive news to be able to control the effect of the privacy breach disclosure on their stock.

A trading strategy based on the mix of breaking news and disclosure laws outperforms the market. In essence, disclosure laws seem to punish breached firms, especially if the disclosure is reinforced by breaking news reports. It may be an indirect way for the FTC to ensure firms are setting the right standards of protection against privacy breaches.

Acknowledgements

I am very grateful to Louis Serranito for excellent research assistance. I appreciate the helpful comments of Alessandro Acquisti, Stephane Bonhomme, Pierre-Andre Chiappori, Victor Lima, John List, Paul Rubin, one anonymous referee, and participants at the APEE conference, CIGO conference, and the George Mason Law School Privacy and Data Security Conference. All remaining mistakes are my own.

References

1. Computer Security Institute/Federal Bureau of Investigation Computer Crime and Security Surveys, 1995-2004, http://www.issa-sac.org/library/index.php? ID=5 (5 February 2015, date last accessed).
2. Miller JL, Craighead CW, Karwan KR. Service recovery: a framework and empirical investigation. *J Oper Manag* 2000;**18**:387–400.
3. Rao S, Griffis SE, Goldsby TJ. Failure to deliver? Link- ing online order fulfillment glitches with future purchase behavior. *J Oper Manag* 2011; **29**:692–703.
4. Lapré MA. Reducing customer dissatisfaction: How important is learning to reduce service failure? *Prod Oper Manag* 2011;**20**:491–507.
5. Hays JM, Hill AV. A preliminary investigation of the relationships between employee motivation/vision, service learning, and perceived service quality. *J Oper Manag* 2001;**19**:335–49.
6. Camp LJ. *Economics of Identity Theft: Avoidance, Causes and Possible Cures*. New York, Berlin: Springer Science & Business Media, 2007.
7. *Wall Street Journal*, http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560? mod=WSJ_hpp_MIDDLENexttoWhatsNewsForth (6 February 2015, date last accessed).

42 Given that those studies were done prior to 2005 and the critical Choicepoint breach establishing a precedent for large fine for privacy breaches, their effect might have been magnified as breaches did not necessarily need to be reported then. As a result of this breach, 22 states ended up enacting consumer privacy laws in 2005, and 43 states are in effect since 2010. Those consumer security breach laws force companies to report breaches to their affected consumers directly.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018

8. Acquisti A, Friedman A, Telang R. Is there a cost to privacy breaches? An event study. In *ICIS 2006 Proceedings* Twenty Seventh International Conference on Information Systems, Milwaukee, 2006.
9. Black EL, Carnes TA, Richardson VJ. The market valuation of corporate reputation. *Corp Reput Rev* 2000;**3**:31–42.
10. Ponemon Institute, Reputation impact of a data breach study, Experian, 2011. https://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf.
11. Cutler DM, Poterba JM, Summers LH. What moves stock prices? *J Portfolio Manag* 1989;**15**:4–12.
12. Mitchell ML, Mulherin JH. The impact of public information on the stock market. *The J Finance* 1994;**49**:923–50.
13. Boudoukh J, Feldman R, Kogan S, Richardson M. Which, news moves stock prices? A textual analysis. No. w18725. National Bureau of Economic Research, 2013.
14. Wasley CE, Wu JS. Why do managers voluntarily issue cash flow forecasts? *J Account Res* 2006;**44**:389–429.
15. Lansford B. Strategic coordination of good and bad news disclosures: The case of voluntary patent disclosures and negative earnings surprises, 2006. Retrieved from SSRN 830705.
16. Rogers JL, Van Buskirk A. Bundled forecasts in empirical accounting research. *J Account Econ* 2013;**55**:43–65. no.
17. Goel S, Shawky HA. Estimating the market impact of security breach announcements on firm values. *Inform Manag* 2009;**46**:404–10.
18. Cohen L, Lou D, Malloy C. Playing favorites: How firms prevent the revelation of bad news. No. w19429. National Bureau of Economic Research, 2013.
19. Hirshleifer D, Lim S, Teoh SH. Driven to distraction: Extra- neous events and underreaction to earnings news. *J Finance* 2009;**64**:2289–325.
20. DellaVigna S, Pollet J. Investor inattention and Friday earnings announcements. *J Finance* 2009;**64**:709–49.
21. Target Press Release. http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance (30 March 2015).
22. Agrawal A, Jaffe JF, Mandelker GN. The post-merger perfor- mance of acquiring firms: a re-examination of an anomaly. *J Finance* 1992;**47**: 1605–21.
23. Conrad J, Cornell B, Landsman WR. When is bad news really bad news? *J Finance* 2002;**57**:2507–2532. no.
24. Campbell R, Al-Muhtadi J, Naldurg P *et al*. Towards security and privacy for pervasive computing. In: *Software Security—Theories and Systems*. Springer Berlin Heidelberg, 2003, 1–15.
25. Cavusoglu H, Mishra B, Raghunathan S. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *Int J Electron Commerce* 2004;**9**:70–104.
26. Hovav A, D'arcy J. The impact of denial-of-service attack announcements on the market value of firms. *Risk Manag Insur Rev* 2003;**6**:97–121.
27. Hovav A, Paul G. The ripple effect of an information security breach event: a stakeholder analysis. *Communications of the Association for Information Systems* 2014;**34**:893–912.
28. Edwards B, Hofmeyr S, Forrest S. Hype and heavy tails: A closer look at data breaches. *J Cybersecurity* 2016;**2**:3–14.
29. Sasha R. Examining the costs and causes of cyber incidents. *J Cybersecurity* 2016;**2**:121–35.
30. Christian B, Eling M, Wirfs JH. Insurability of cyber risk: an empirical analysis. *The Geneva Papers* 2015;**40**:131–58.
31. Cameron AC, Gelbach JB, Miller DL. Robust inference with multiway clustering. *J Bus Econ Stat* 2011;**29**:238.
32. Gelbach JB, Helland E, Klick J. Valid inference in single-firm, single-event studies. *Am Law Econ Rev* 2013;**15**:495–541.
33. Conley T, Taber C. Inference with difference in differences with a small number of policy changes. *Rev Econ Stat* 2011;**93**:113–25.
34. Yayla AA, Hu Q. The impact of information security events on the stock value of firms: The effect of contingency factors. *J Info Technol* 2011;**26**: 60–77.
35. Jarrell G, Peltzman S. The impact of product recalls on the wealth of sellers. *J Political Econ* 1985, **93**:512–36.
36. Dowdell TD, Govindaraj S, Jain PC. The Tylenol incident, ensuing regulation, and stock prices. *JFQA* 1992;**27**:283–301.
37. Jory SR, Ngo T, Wang D, Saha A. The market response to corporate scandals involving CEOs. *Appl Econ* 2015; 1–16.

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/3/2/91/4775012
by guest
on 02 July 2018